16-1301SAG

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Christine D. Carlson, a Special Agent (SA) with the Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), being duly sworn, depose and state that:

1. I have been an Agent since June 1996. As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A. I have gained experience through training in seminars, classes, and daily work related to conducting these types of investigations. Specifically, I have received formal training through U.S. Customs, HSI, and other agencies in the area of child pornography, pedophile behavior, collectors of other obscene material, and internet crime. I have participated in the execution of numerous search warrants, which involved child exploitation and/or child pornography offenses. Many of the child exploitation and/or child pornography search warrants resulted in the seizure of computers, cell phones, magnetic storage media for computers, other electronic media, and other items evidencing violation of federal laws, including various sections of Title 18, United States Code, Section 2252A involving child exploitation offenses. I have also participated in the execution of numerous search warrants for online accounts, such as email accounts, online storage accounts and other online communication accounts related to child exploitation and/or child pornography. In the course of my employment with HSI, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media and within online accounts.

2. As a federal agent, I am authorized to investigate violations of laws of the United

States and I am a law enforcement officer with the authority to affect arrests and execute warrants issued under the authority of the United States.

3. This affidavit is being submitted in support of applications for warrants to search a desktop computer, a netbook, a microSD card, and a cell phone located at the offices of the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations, 40 South Gay Street, Baltimore, Maryland, and seized from the residence of Michael K. WATERS, 309 Raleigh Road, Glen Burnie, Maryland 21061. These items were seized pursuant to a state search and seizure warrant issued by the Honorable Judge Wilson of the District Court for Baltimore County, State of Maryland (copy of the said search and seizure warrant is attached hereto and incorporated herein by reference as Attachment D). These items are to be searched for evidence of violations of Title 18, United States Code, Section 2252A(a)(2)(distribution and receipt of child pornography), and Title 18, United States Code, Section 2252A(a)(5)(B)(possession of child pornography).

4. The statements in this affidavit are based in part on information provided by detectives of the Baltimore County Police Department and Special Agents of HSI, as well as documents and reports prepared by detectives of the Baltimore County Police Department, and on my experience and background as a Special Agent of HSI. Since this affidavit is being submitted for the limited purpose of securing search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probably cause to believe that evidence, fruits, and instrumentalities of the violations of Title 18, United States Code, Section 2252A(a)(2)(distribution and receipt of child pornography), and Title 18, United States Code, Section 2252A(a)(5)(B)(possession of child pornography) are located within the desktop computer, netbook, microSD card, and cell phone

seized from the residence of Michael K. WATERS, 309 Raleigh Road, Glen Burnie, Maryland 21061.

SUMMARY CONCERNING CHILD PORNOGRAPHY, PERSONS WHO POSSESS AND COLLECT CHILD PORNOGRAPHY AND HOW USE OF COMPUTERS AND THE INTERNET RELATES TO THE POSSESSION, RECEIPT AND DISTRIBUTION OF CHILD PORNOGRAPHY

5. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who utilize the internet to view and receive images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals, including the following:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers and in online storage, email accounts or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer to Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

6. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers and the internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography.

d. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

e. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo! and Google, Inc., Facebook, Dropbox, Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including email, images, videos, and other files. The data is maintained on the servers of the providers, and is occasionally retained by the providers after the user deletes the data from their account.

f. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

7. Based on traits shared by collectors, the use of email, online storage accounts, and other online communication accounts, and the increased storage capacity of computers and server space over time, there exists a fair probability that evidence regarding the distribution, receipt and possession of child pornography will be found in the desktop computer, netbook, microSD card, and cell phone seized from the residence of Michael WATERS, notwithstanding the passage of time.

PEER-TO-PEER FILE SHARING

8. A growing phenomenon on the Internet is peer-to-peer file sharing (hereinafter "P2P"). P2P is a method of file sharing available to Internet users through the use of special software that allows users to trade digital files through P2P networks formed by linking computers together through the Internet. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files(s) on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer and conducting a search for files that are currently being shared on the network. Some types of P2P software set up their searches by keyword. The results of the keyword search are displayed to the user. The user then selects files(s) from the results for download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer containing the file.

9. For example, a person interested in obtaining visual depictions of minors engaged in sexually explicit conduct would open the P2P application on his/her computer and, using a term such as "preteen sex," conduct a search of a P2P network for computers sharing files associated with that term. The user can then select files from the search results and download them directly from the computer(s) sharing those files. The download of a file occurs through a

direct connection between the computer requesting the file and the computer(s) hosting the file. Once a file has been downloaded, it is stored on the requesting user's computer in the area previously designated by the requesting user and will remain there until moved or deleted.

10. One of the advantages of P2P file sharing is that a user can download multiple files in parallel. This means that a user can download more than one file at a time. In addition, a user can download parts of one file from more than one source computer at a time. For example, a user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that is reduces the time it takes to download a file.

11. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

FACTS AND CIRCUMSTANCES OF THE INVESTIGATION

12. On March 6, 2016, a detective from the Baltimore County Police Department, working in an undercover capacity, used a computer to connect to the Internet to conduct an online investigation into the sharing of child pornography on the P2P file sharing network known as BitTorrent. The detective located an IP address 96.244.190.218 associated with a torrent file with an infohash[1] that was identified as being a file of investigative interest to child pornography investigations.

13. Using a computer running investigative BitTorrent software, the detective directly connected to the device at IP address 96.244.190.218. The device reported it was using BitTorrent client software –UT340B- uTorrent 3.4.

[1] An infohash is a unique mathematical algorithm for the contents of a torrent.

14. On March 6, 2016, between 0901hrs EDT and 0923hrs EDT, the detective successfully completed a partial download of a video that the device at IP address 96.244.190.218 was making available. The device at IP address 96.244.190.218 was the sole candidate for the download, and as such, the file was downloaded directly from IP address 96.244.190.218. I subsequently reviewed the one video file and concluded, based on my training and knowledge, that the one video file contained a visual depiction of a minor engaging in sexually explicit conduct and is child pornography as defined under 18 U.S.C. § 2256(8). In the one video, the title of which is "Nablot Sucker [3.30m].avi," a prepubescent male is performing oral sex on an adult.

15. A public database query determined that IP address 96.244.190.218 was managed by Verizon. Verizon provided records which established that on March 6, 2016 between 0901hrs EDT and 0923hrs EDT, the period of the download of the relevant file, the IP address 96.244.190.218 was assigned to: Serena Black, 102 Shipway, Dundalk, MD 21222, telephone#: 443-825-2226, primary username: busseewall@yahoo.com.

16. On March 15, 2016, a search and seizure warrant for Black's residence, 102 Shipway, Dundalk, Maryland, was applied for and granted by the Honorable Judge Tirabassi of the Baltimore County District Court.

17. On March 17, 2016, the search warrant for Black's residence was executed by detectives from the Baltimore County Police Department. Only Serena Black, born 1959, was present during the execution of the search warrant.

18. Ms. Black was advised of her rights per *Miranda* and stated that she understood her rights and agreed to be interviewed by detectives. Ms. Black informed detectives that she had one working computer in her home and one smartphone. Ms. Black advised that she lives

alone however her son, Michael WATERS, had just been released from jail on March 4, 2016 and had come to stay with her from March 4th through March 6th. Ms. Black further advised that when WATERS arrived at her residence, after being released from jail, that she gave him an LG cell phone, which was not activated for cellular use, but still had the capability to access the internet and use wi-fi. Ms. Black advised that after she gave WATERS the phone, WATERS asked her for the wi-fi password for her home router, which she gave to him. Ms. Black stated that WATERS left her residence on March 6, 2016 with the LG cell phone. Ms. Black stated she did not know where her son was staying and did not have any way of getting in touch with him. Ms. Black also did not know if WATERS was on parole or probation.

19. Investigators conducted a forensic triage of Ms. Black's desktop computer and did not find any evidence of child pornography on it, nor did it have any type of file sharing software installed on it.

20. A couple of hours after detectives left Ms. Black's residence, Ms. Black contacted one of the interviewing detectives and informed him that she had not been honest with him. Ms. Black told the detective that she knew exactly where her son was and advised that her son was staying with her father, Eddie Ward, at 309 Raleigh Road, Glen Burnie, Maryland. Ms. Black went on to say that she had just visited her son at this address on March 15, 2016, and at that time he still had the LG cell phone that she had given him when he got out of jail.

21. On March 17, 2016, detectives from Baltimore County Police Department responded to 309 Raleigh Road, Glen Burnie, Maryland and met with Michael WATERS. WATERS was informed of the investigation at his mother's house. Initially, WATERS believed that detectives were there to arrest him for not checking in with his probation agent. WATERS advised that he had just been released from jail on March 4, 2016 and failed to check in with his

probation agent. WATERS was advised by detectives that he was not under arrest and that detectives were there to talk with him about the cell phone that his mother had given him when he got out of jail. WATERS confirmed that his mother had given him a cell phone after his release and he had used it to connect to the wi-fi at her residence. WATERS then stated that he had lost the phone on the light rail the day before. WATERS told detectives that he had another cell phone inside the residence and asked if he could go in and get it. Detectives advised WATERS that he could go inside the residence and retrieve his cell phone. WATERS went inside the residence by himself while detectives waited outside. WATERS returned with a cell phone that was not powered on and had a cracked screen. It was apparent to detectives that WATERS was not telling the truth. WATERS then changed his story and told detectives that he had sold the cell phone his mother had given him for $80 and used the money to buy a gram of cocaine. WATERS advised that he did not check in with his probation agent because he had snorted the entire gram of cocaine. When detectives asked direct and specific questions about the cell phone WATERS had been given by his mother, WATERS admitted that the cell phone was inside the residence at 309 Raleigh Road, Glen Burnie, Maryland. WATERS admitted to using a torrent program on the phone and downloading child pornography to the phone. When asked if WATERS had any computers inside 309 Raleigh Road, Glen Burnie, Maryland, WATERS advised that he had an old computer that does not work and was put away. A detective went to the front door of the residence to speak with WATER'S grandfather, Eddie Ward. Mr. Ward is elderly and invited the detective inside the residence and to sit down in his living room. The detective noticed a laptop computer on a table with the lid open and thumb drive plugged into it. The detective advised Mr. Ward of the nature of the investigation and that his residence was going to be secured pending the issuance of a search and seizure warrant. Mr.

Ward advised that he is computer illiterate and the laptop belonged to his grandson Michael, and that Michael had been using it.

22. On March 17, 2016 at approximately 1126hrs EDT, Detective Rees obtained a search and seizure warrant for the residence located at 309 Raleigh Road, Glen Burnie, Maryland. The search warrant was signed by the Honorable Judge Wilson of the District Court of Baltimore County, State of Maryland (copy of the said search and seizure warrant is attached hereto and incorporated herein by reference as Attachment C).

23. When Sgt. Smith advised WATERS that a search and seizure warrant had been signed for his residence, WATERS advised that the LG cell phone was in the cat litter box in his bedroom. A search of the cat litter box revealed the LG cell phone, taken apart, and the microSD card removed. Further search of the litter box revealed a Verbatim 16GB microSD card. Upon Detective Rees' return to the residence, WATERS advised Detective Rees that he wished to speak with him again. Detectives and WATERS walked to a pavilion at the park located at the end of Raleigh Road. Detectives interviewed WATERS at a picnic table and the interview was audibly recorded. WATERS was advised of his right under Miranda, which he stated he understood and waived. WATERS stated the reason he wasn't honest from the beginning was because he was afraid to go back to jail. WATERS advised he left the cat litter scoop in the litter box because he knew that detectives would be getting the phone out of the litter. WATERS advised the phone had a microSD card in it when his mother gave it to him, but stated he had switched it out with another microSD card that had larger storage capacity and may have dropped the other microSD card in the park over by the playground. Detective Kaczynski searched the area by the playground and did not find a microSD card. WATERS stated that when he got out of jail, his mother gave him the cell phone and he asked her for her wi-fi

password. WATERS stated he connected to his mother's wi-fi and downloaded bit torrent file sharing software onto the phone. WATERS further admitted to downloading the video "Nablot Sucker" at his mother's home. WATERS described the video as a 9-10 year old kid "giving head." WATERS later admitted to downloading the same video again because he had deleted the first one. WATERS admitted to walking around the neighborhood with the phone looking for open wi-fi. WATERS admitted to being involved with child pornography prior to his most recent incarceration and estimated he first saw child pornography five years ago. WATERS admitted to using the following search terms when searching for images and videos of child pornography: PTHC, babyj, and cbaby along with typing in ages. WATERS explained how the BitTorrent file sharing network works using the terms such as "peers" and "seeding." WATERS also stated that he had hooked his phone up to the laptop inside his residence at 309 Raleigh Road, Glen Burnie, Maryland and had recently viewed child pornography.

24. An on-scene forensic triage of the Verbatim 16GB microSD card located in the cat litter box revealed over 100 images and videos depicting children engaged in sexually explicit conduct. One of the videos located on the Verbatim 16GB microSD card is the video described in paragraph 14 above.

25. The following is a description of the items seized from the residence located at 309 Raleigh Road, Glen Burnie, Maryland pursuant to the state warrant and the subject of this affidavit and search warrant:

- *Dell Inspiron 660S desktop computer, sn: 3Z46CX1*
- *EZ Book PC-7" Netbook, sn: BS03081072A000607*
- *Verbatim 16GB microSD card*
- *LG camera cell phone*

26. The items listed in paragraph 25 above were seized by Baltimore County Police Department and subsequently turned over to me.

16-1301SAG

27. Even though a member of the Baltimore County Police Department obtained a search warrant for the residence, it should be noted that as of the date of this application, neither I, nor any other federal agent, has attempted to inspect, review, copy and/or search said evidence in any manner whatsoever. Based on the advice of Assistant United States Attorney Zachary Myers, and out of an abundance of caution, I am applying for the issuance of a federal search warrant as a prerequisite to any forensic search or analysis of the items described in Attachment A.

CONCLUSION

28. Based on the foregoing, I respectfully submit that there is probable cause to believe that the aforementioned federal statutes have been violated and that there is probable cause to believe that evidence of these crimes can be found on the computers, cell phones, and other storage devices seized from the residence of Michael WATERS, and currently stored by Homeland Security Investigations in their offices located in Baltimore, Maryland.

29. WHEREFORE, I respectfully request that this Court issue search warrants to search the items described in Attachment A, which is incorporated herein by reference, and to seize any items located pursuant to the search as described in Attachment B which is also incorporated herein by reference.

Christine D. Carlson
Special Agent
Homeland Security Investigations

Subscribed to and sworn before
me this 17th day of May, 2016

THE HONORABLE Stephanie A. Gallagher
UNITED STATES MAGISTRATE JUDGE

16-1301SAG

ATTACHMENT A

DESCRIPTION OF ITEMS TO BE SEARCHED

The following is a list of items seized from 309 Raleigh Road, Glen Burnie, Maryland 21061.

- *Dell Inspiron 660S desktop computer, sn: 3Z46CX1*
- *EZ Book PC-7" Netbook, sn: BS03081072A000607*
- *Verbatim 16GB microSD card*
- *LG camera cell phone*

16-1301SAG

ATTACHMENT B
LIST OF ITEMS TO BE SEIZED

The items in Attachment A may be searched for the following items, which may be seized:

All records, documents, items, data and other information that may constitute fruits or instrumentalities of, or contain evidence related to, violation of Title 18 U.S.C. §§ 2252A(a)(2), and 2252A(a)(5)(B) including, but not limited to, the following:

1. Any and all notes, documents, records, or correspondence pertaining to child pornography as defined under Title 18, United States Code, Section 2256(8).

2. Any and all correspondence identifying person transmitting, receiving or possessing, through interstate commerce including by U.S. Mails or by computer, any visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(a).

3. Any and all records, documents, invoices and materials that concern any online accounts, including Internet Service Providers, social networking sites, screen names or email accounts.

4. Any and all visual depictions of minors.

5. Any and all documents, records, or correspondence pertaining to occupancy or other connection to 309 Raleigh Road, Glen Burnie, Maryland.

6. Any and all diaries, notebooks, notes and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

7. Any and all diaries, notebooks, notes, pictures, chats, directions, maps, banking, travel, documents, and any other records reflecting personal contact and any other activities with minors.

8. Any and all notes, documents, records, photos or correspondences that relate to travel.

9. Any and all notes, documents, records, photos or correspondence that indicate a sexual interest in children, including, but not limited to:

a. Correspondence with children;
b. Any and all visual depictions of minors;
c. Internet browsing history;
d. Books, logs, diaries and other documents.

As used above, the terms "records, documents, messages, correspondence, data and materials" includes records, documents, messages, correspondence, data, and materials, created, modified or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of a computer, hardware, software, documentation, passwords, and/or data security devices.

10. Evidence of who used, owned, or controlled the computer and/or media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contact, "chat," instant messaging logs, photographs, and correspondence;

a. Evidence of software that would allow others to control the computer and/or media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
b. Evidence of the lack of such malicious software;
c. Evidence of the attachment to the computer and/or media of other storage devices or similar containers for electronic evidence;
d. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer and/or media;
e. Evidence of the times the computer and/or media was used;
f. Passwords, encryption keys, and other access devices that may be necessary to access the computer and/or media;
g. Documentation and manuals that may be necessary to access the computer and/or media or to conduct a forensic examination of the computer and/or media;
h. Contextual information necessary to understand the evidence described in this attachment.

Any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment, including floppy diskettes, fixed hard disks, or removable hard disk cartridges, software or memory in any form. The search procedure of the electronic data contained in computer operating software or memory devices shall include the following techniques which shall be used to minimize the risk that those conducting the search will view information not within the scope of the warrant:

a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;
c. "scanning" storage areas to discover and possibly recover recently deleted files;
d. "scanning" storage areas for deliberately hidden files; or

e. performing key word or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

11. If after performing these procedures, the directories, files or storage areas do not reveal evidence of child pornography or other criminal activity, the further search of that particular directory, file, or storage area shall cease.

16-1301SAG

DISTRICT COURT OF MARYLAND
FOR BALTIMORE COUNTY

APPLICATION AND AFFIDAVIT FOR SEARCH AND SEIZURE WARRANT

To the Honorable Judge D Wilson of the District Court for Baltimore County,

Your affiant, Detective J. Rees #4648, a member of the Baltimore County Police Department, being duly sworn, knows through his training, knowledge, and experience that subjects engaging in the distribution, purchase, receipt, sale or trade of child pornography will frequently make use of computer equipment and video production equipment to further their activity. Computers, Internet services and storage devices enable subjects engaging in the distribution, purchase, receipt, sale or trade of child pornography to communicate with co-conspirators in any region or country with the perception of anonymity. The copying of child pornography on DVD/CD'S and other storage devices is a way to trade the child pornography easily and to save the child pornography to view again at a later date. Subjects who view or collect child pornography retain their assortment for long periods of time and value their collections, often going to great lengths to organize and protect their collections, including concealing the images on computer media and other storage devices. Your affiant also knows through his training, knowledge, and experience that when subjects possessing child pornography conceal or delete it to avoid detection, that it is possible to recover files and data from computer media in hidden areas or after it has been deleted.

Your affiant, being duly sworn, deposes and says that he has reason to believe that:

ON THE PREMISES KNOWN AS:

309 Raleigh Road Glen Burnie, MD 21061 (Anne Arundel County)

Described as:
A single family residence with gray siding, black shutters, and a white front door. There are no numerical markings on the home, however it is situated directly between houses marked 311 and 307. The residence is currently secured by Baltimore County Police Detectives and is known by sight to your Affiant.

there is presently concealed certain property, NAMELY:

A. Seize and examine any and all cell phones
B. Seize any documents, envelopes, cancelled checks, or papers in the name of occupants that establishes occupancy.
C. Seize and examine address books, advertisements, brochures, catalogs, correspondence, documents, electronic organizers, mailing lists, notes, organizers, publications, receipts, records that may indicate the distribution, barter, purchase, receipt, sale or trade of child pornography.
D. Seize and examine any documents, notes, papers or other items containing chat logs, E-mail addresses, E-mail messages, Internet Service Provider information, IP addresses, passwords, Uniform Resource Locator addresses and user profiles.
E. Seize and examine any books, DVD, magazines, motion picture film of any format, negatives, photographs, printed images generated by computer, slides, undeveloped film of any format and videocassettes that may contain child pornography.
F. Seize and examine any electronic media including, but not limited to Media Cards and Flash Based memory that may contain evidence of the distribution, production, receipt, transmission or viewing of child pornography stored in any format.
G. Seize and exam any and all portable media players (PMP), a consumer electronics device that is capable of storing and playing digital media. The digital media is typically stored on a hard drive, microdrive, or flash memory. PMPs are capable of supporting digital audio, digital images, and digital video. Usually, a color liquid crystal display (LCD) or organic light-emitting diode (OLED) screen is used as a display. Various players include the ability to record video, usually with the aid of optional accessories or cables, and audio, with a built-in microphone. Some players include readers for memory cards, which are advertised to equip players with extra storage or transferring media.

H. Seize and examine any magnetic media including, but not limited to hard drives, floppy diskettes and tapes of any format that may contain evidence of the distribution, production, receipt, transmission or viewing of child pornography stored in any format.
I. Seize and examine any optical media including, but not limited to CD's, DVD's and Blu-rays of any format that may contain evidence of the distribution, production, receipt, transmission or viewing of child pornography stored in any format.
J. Seize and examine any computer hardware capable of analyzing, collecting, concealing, converting, displaying, receiving or transmitting data electronically, magnetically or optically. This hardware includes, but is not limited to central processing units, portable computers (i.e. laptop computers), file servers, peripheral input/output devices (i.e. keyboards, plotters, pointing devices, printers, scanners and video display monitors), storage devices capable of reading and/or writing to computer media (i.e. electronic, magnetic or optical), communications devices (i.e. modems, cable modems, network adapters and wireless communication devices),

any devices or parts used to restrict access to computer hardware (i.e. keys and locks) and any other piece of equipment necessary to duplicate the functionality of the hardware at the time of seizure (i.e. batteries, cables, instruction manuals and power cords) that may be used in the distribution, production, receipt, transmission or viewing of child pornography.

K. **Seize and examine any computer software stored electronically, magnetically, or optically that may be used to facilitate the distribution, production, receipt, transmission or viewing of child pornography and any instruction manuals associated with the software.**

L. **To seize and examine any cameras, digital cameras, motion picture cameras, video cameras, web cameras and any associated accessories (i.e. backdrops, batteries, carrying cases, instruction manuals, lenses, lighting equipment, meters, remote controls and tripods) that may be used in the production of child pornography.**

M. **Open any containers, envelopes, boxes, packages, safes to examine the contents and seize any of the aforementioned items,**

which is evidence relating to the commission of the crime of Child Pornography in violation of in violation of Maryland Annotated Code, Criminal Code, Article CR 11-207 and 11-208. The fact tending to establish grounds for the issuance of a Search and Seizure Warrant are set forth in the below Affidavit.

AFFIDAVIT OF PROBABLE CAUSE

Peer to Peer (P2P) file sharing allows people using P2P software to download and share files with other P2P users using the same or compatible P2P software. P2P software is readily available on the Internet and often free to download. Internet connected devices such as computers, tablets and smartphones running P2P software form a P2P network that allow users on the network to share digital files. BitTorrent is one of many P2P networks. For a user to become part of the BitTorrent network, the user must first obtain BitTorrent software and install it on a device. When the BitTorrent software is running and the device is connected to the Internet, the user will be able to download files from other users on the network and share files from their device with other BitTorrent users.

Users of the BitTorrent network wishing to share new content will use a BitTorrent program to create a "torrent" file for the file or group of files they wish to share. A torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Torrent files are typically found as the result of keyword searches on Internet sites that host or link to them. Torrent files may be referenced by their "infohash", which uniquely identifies the torrent based on the file(s) associated with the torrent file.

To download file(s) from other users on the BitTorrent network, a user typically obtains a torrent file. The BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts or the actual file(s) being sought. The download of the content referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

On Sunday, March 06, 2016, Det. Rees was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. Det. Rees directed his investigative focus to a device at IP address 96.244.190.218, because it was associated with a torrent with the infohash: c0d603788a4c1a5850253f53a3d2c44a3478fe6a. This torrent file references 1 file, which was identified as being a file of investigative interest to child pornography investigations.

Using a computer running investigative BitTorrent software, Det. Rees directly connected to the device at IP address 96.244.190.218, hereinafter referred to as "Suspect Device". The Suspect Device reported it was using BitTorrent client software -UT340B- uTorrent 3.4

On Sunday, March 06, 2016, between 0901 hrs and 0923 hrs, Det. Rees completed a partial download of the following file that the device at IP address 96.244.190.218 was making available:

Nablot Sucker [3.30m].avi

Description: This file is a video depicting a young male child who appears to be approximately 6-9 years old. The child is seen performing oral sex on an adult male's penis throughout the duration of the video.

Det. Rees recognizes through his training, knowledge, and experience that the files described above are child pornography.

The device at IP Address 96.244.190.218 was the sole candidate for the download, and as such, the file was downloaded directly from this IP Address.

A check of publicly available records located online by an organization known as the American Registry of Internet Numbers, determined that the aforementioned I.P. address was assigned to Verizon. A Grand Jury Subpoena was issued for the aforementioned IP address at the dates and times the child pornography was downloaded.

A subpoena was sent to Verizon requesting information, including the subscriber name and address, for IP address 96.244.190.218 for the date and time of the downloads. The information received from Verizon is as follows:

Subscriber Name:	Serena Black
Service address:	102 Shipway Dundalk, MD 21222
Telephone #:	443-825-2226
Primary username:	busseewall@yahoo.com

Based on the aforementioned investigation Det. Rees prepared a search and seizure warrant for 102 Shipway Dundalk, MD 21222. The warrant was signed by the Honorable Judge Tirabassi on 03/15/2016 at 1103 hours.

The valid search and seizure warrant was served on 03/17/2016 at 0435 hours. Entry was gained without force when Serena Black opened the door pursuant to Det. Rees knocking and announcing. The following residents were home at the time of the warrant service:

- Serena Black f/b 05/11/1959

The following officers were present for the service of the warrant:

- Sgt. Smith #4159 (Supervisor)
- Det. Rees #4648 (Affiant/Forensics/Interview)
- Det. Raut #4438 (Forensics)
- Det. Kaczynski #3425 (Interview)
- Det. Childs #4505 (Inventory)
- Det. Adamski #4657 (Photos)
- Det. Maisano #5120 (Sketch)
- Lt. Wiedeck #3480 (Security)

Det. Rees read the warrant aloud to the Ms. Black. Det. Rees then advised her of her rights per Miranda, which she stated she understood. Det. Rees learned that the home has a password protected wireless network. Det. Rees asked about computers in the home. Det. Rees learned that Ms. Black has 1 functioning computer in her home and 1 smart phone.

Det. Rees utilized the forensic triage tool OS Triage to scan Ms. Black's Dell computer. The computer did not have any evidence of child pornography on it, nor did it have any type of file sharing software installed on it.

Detectives Rees and Kaczynski interviewed Ms. Black. The interview was conducted in private and was audibly recorded. Det. Rees advised Ms. Black of her Rights per Miranda for a second time. Again, she stated that she understood her rights and agreed to be interviewed. Ms. Black advised that she lives alone, however her son, Michael Waters, was released from prison on March 4th and came to stay with her from March 4th-6th. She further advised that when he got to her house she gave him an LG smart phone, which while not activated with cellular service, still had the ability to access and use wi-fi. She further advised that when she gave him the phone he asked her for her wi-fi password for her home router, which she gave him. It should be noted that the date child pornography was shared with Det. Rees from Ms. Black's home was March 6th around 0900 hours in the morning. Ms. Black advised that her son left her home on March 6th in the afternoon hours. Ms. Black told Det. Rees that she had no idea where her son is staying nor did she have any way to get in touch with him. She advised that she did know that he is on either Parole or Probabtion.

A criminal record check of Michael Kennell Waters found that he was just released from prison after being convicted of 2nd Degree Child Abuse.

A couple of hours after Detective Rees left Ms. Black's home he received a phone call from her. She advised that she had not been honest with Det. Rees and that she knew exactly where her son is. She advised that he is staying with her father, Eddie Ward, at 309 Raleigh Road Glen Burnie, MD 21061 and that she had just visited Michael there on 03/15/2016. She further advised that he still had the phone she gave him.

On 03/17/2016 at approximately 0920 hours, Sgt. Smith along with Detectives Rees, Raut, and Kaczynski responded to 309 Raleigh Road. When the Detectives arrived, Michael Waters opened the front door of 309 Raleigh Road and walked out to the street. Detectives Rees and Kaczynksi met with Mr. Waters in front of 309 Raleigh Road while Sgt. Smith and Det. Raut stayed at their vehicles. Det. Rees spoke with Mr. Waters regarding the investigation at his mother's house. Initially, he believed the Detectives were there to arrest him for not checking in with his Probation Agent. Mr. Waters advised that he was just released from prison on 03/04/2016 and failed to check in with his Probation Agent when he was supposed to do so. Det. Rees informed him that he was not under arrest and spoke with him regarding the phone his mother gave him. He acknowledged and confirmed that his mother gave him a smart phone when he got to her house after being released. He advised that he connected to her wi-fi with it. He then explained that he lost it yesterday while riding the light rail. He gave a story about switching light rail cars and leaving it on a seat. He then advised that he had another phone inside of the house and asked Det. Rees if he could go and get it. Det. Rees advised him that he could. Mr. Waters went into 309 Raleigh Road by himself while the Detectives waited out front in the street. He returned a short time later with a phone that was not powered on and had a cracked screen. As the interview progressed it was apparent that Mr. Waters was not being truthful about the phone his mother gave him.

He then changed his story and advised that he sold the phone yesterday for $80 and used the money to buy a gram of Cocaine. He advised that he did not check in with his Probation Agent because he snorted the entire gram of Cocaine. When he was asked direct and specific questions about selling the phone he admitted that the phone was actually inside of 309 Raleigh Road. He then admitted that he had used a torrent program on the phone and that he had downloaded Child Pornography to the phone. Mr. Waters was asked about other computers in 309 Raleigh Road that either belong to him or that he uses. Det. Rees asked this because Det. Rees knows through his training, knowledge, and experience that it is very easy and very common for smart phone users to back up and/or sync their phones to a computer wither to reduce storage space on their phone or to save files that are important to them. Mr. Waters advised that he has an old computer in the home, however it does not work and was put away.

Det. Rees went to the front door of the home to speak with Mr. Waters' grandfather, Eddie Ward. It should be noted that Mr. Ward is elderly. Mr. Ward answered the door and asked Det. Rees to come in and sit down in his living room. As soon as Det. Rees stepped into the house he noticed a laptop computer on a table with the lid open and a thumb drive plugged in to it.

Det. Rees explained to Mr. Ward that his house was being secured for a search & seizure warrant along with the nature of the investigation. Mr. Ward advised that he does not have any computers and that he is computer illiterate. He then pointed to the laptop and advised that it belongs to his grandson, Michael, and that Michael has been using it.

Based on the numerous untrue and deceptive statements made by Mr. Waters to the Detectives regarding the phone given to him and his use of a computer Det. Rees believes it is probable that Mr. Waters is attempting to hide or conceal his involvement with Child Pornography and devices that contain evidence of Child Pornography. Det. Rees knows through his training, knowledge, and experience that it is very easy and very common for smart phone users to back up and/or sync their phones to a computer wither to reduce storage space on their phone or to save files that are important to them. Det. Rees has investigated several cases where a suspect has downloaded child pornography to a smartphone or other mobile device then synced that device with a computer and/or saved child pornography to a removable storage device like a thumb drive.

Your affiant submits based on the facts set forth in this affidavit, that there is probable cause to believe that a user of a device/computer located **309 Raleigh Road Glen Burnie, MD 21061** has child pornography that was shared on the Bittorrent P2P network.

Finally, based upon the conduct of individuals involved in the possession of child pornography at the location set forth above, forensic examiners can recover files even when they have been deleted. Detective Rees has investigated cases where forensic examiners recovered deleted files which had been deleted for several months. When the computer which was sharing the child pornography is seized, it is likely to contain evidence relating to the possession and/or distribution of child pornography even if the child pornography has been deleted.

Based on the above information, there is probable cause to believe that the Child Pornography laws of Maryland have been violated, and that the property, evidence, and instrumentalities of these offenses, listed in the items to be searched for and seized if found, are located **309 Raleigh Road Glen Burnie, MD 21061.**

EXPERTISE

Your Affiant, Detective Rees, has been a member of the Baltimore County Police Department since June of 2001. During this time your Affiant has received extensive training in the following areas: the preparation and execution of Search and Seizure warrants, the recognition and collection of evidence, constitutional law, and proper arrest procedures.

Your Affiant attended and successfully completed The Baltimore County Police Academy from June 2001 through November 2001. In November 2001, your affiant was assigned to Precinct 1, Wilkens, as a Patrol Officer. During this time your affiant made hundreds of criminal arrests and assisted with the execution of several search and seizure warrants. Your affiant has also recognized and collected evidence on numerous occasions and has made numerous criminal arrests while assigned to the Criminal Investigations Division. Your affiant has also attended numerous training courses while working as a member of the Baltimore County Police Department. The following are training courses relevant to Det. Rees' current assignment in the Crimes Against Children Unit.

- Attended 2015 Florida ICAC Conference
- NW3C – Cybercop 225 – Apple iDevice Forensics
- NW3C – Cybercop 215 – Macintosh Triage and Imaging
- ICAC Emule Investigations
- Attended 2014 Florida ICAC Conference
- Attended 2014 Techno Security & Mobile Forensics World Conference
- ICAC Bit Torrent Investigations
- NW3C – Cybercop 201 – Intermediate Data Recovery and Acquisition
- Attended 2012 National Law Enforcement Training on Child Expolitation Atlanta, GA
- Roundup Ares (ICAC-Internet Crimes Against Children Task Force)
- osTriage:On-Scene Preview Tool (ICAC-Internet Crimes Against Children Task Force)
- Forensic Artifacts in P2P Investigations (ICAC-Internet Crimes Against Children Task Force)
- NW3C – Cybercop 101 – Basic Data Recovery and Acquisition
- NW3C – Cyber Investigation 101 – Secure Techniques for Onsite Preview

- ICAC Task Force – Gigatribe Peer to Peer Investigations (ICAC-Internet Crimes Against Children Task Force)

- Attended the 2011 Crimes Against Children Conference in Dallas, TX

- ICAC task Force – Roundup for P2P Investigators (ICAC-Internet Crimes Against Children Task Force)

- The Reid Technique of Interview & Interrogation for Child Abuse Investigations (John Reid & Associates)

- ICAC Task Force – Undercover Chat Investigations (ICAC-Internet Crimes Against Children Task Force)

- FBI-CART ImageScan System version 3 (Federal Bureau of Investigation)

- ICAC Task Force - Investigative Techniques Training (ICAC-Internet Crimes Against Children Task Force)

- Protecting Children Online: Technology Facilitated Crimes Against Children (National Center for Missing and Exploited Children)

- Finding Words (Maryland Police and Correctional Training Commission)

- Innocent Images Training (Federal Bureau of Investigation)

- Advanced Course in The Reid Technique of Interview & Interrogation (John Reid & Associates)

- The Reid Technique of Interview & Interrogation (John Reid & Associates)

- Search and Seizure Seminar (Baltimore County Police)

- Basic Criminal Investigator School (Baltimore County Police)

- Interview and Interrogation School (Multijurisdictional Counterdrug Task Force)

In June 2007, your affiant was assigned to the Criminal Investigations Division, Violent Crimes Unit. Your affiant successfully conducted and completed numerous criminal investigations while serving as a Detective in the Violent Crimes Unit. Your affiant prepared numerous Search & Seizure warrants while in the Violent Crimes Unit resulting in the seizure of evidence used to successfully prosecute Attempted Murder and Firearms related cases.

In March 2008, your affiant was assigned to the Criminal Investigations Division, Crimes Against Children Unit. Your affiant was assigned to the Sexual Child Abuse Squad. Your affiant has successfully conducted and completed numerous Sexual Child Abuse investigations while serving as a Detective in the Crimes Against Children Unit. Your affiant then became cross trained in the investigation of Child Pornography and Sexual Exploitation of Children.

While in the Crimes Against Children Unit your affiant has attended several specialized training modules presented by the FBI, ICAC Task Force, National White Collar Crime Center, and the National Center for Missing and Exploited Children. These training modules have trained Det. Rees in the use of undercover means to investigate the sexual exploitation of children by way of the Internet. Your affiant has successfully conducted and completed numerous Child Pornography and Sexual Exploitation investigations. Your affiant has written well over 100 search & seizure warrants related to Sexual Abuse and Child Pornography investigations. During those investigations, your affiant has identified and recovered child pornography evidence. Your affiant has interviewed hundreds of suspects relating to sexual crimes against children, both hands on offenders and those utilizing online means.

Your Affiant is also a Task Force Officer (TFO) with the FBI and is assigned to the Maryland Child Exploitation Task Force.

THE USE OF PEER-TO-PEER FILE SHARING SOFTWARE TO DISTRIBUTE CHILD PORNOGRAPHY ON THE BITTORRENT NETWORK

P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software from a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. Bittorrent, one type of P2P software, sets up its searches by keywords typically on torrent websites. The results of a keyword search are displayed to the user. The website does not contain the files being shared only file referred to as a "torrent". The user then selects a .torrent file(s) from the results for download. This .torrent file contains instructions on how a user can download the file(s) referenced in the Torrent.

The download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) sharing the actual files (not the torrent file but the actual files referenced in the .torrent file using any bittorrent client.)

For example, a person interested in obtaining child pornographic images would open the bittorrent website on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The results of the search are returned to the user's computer and displayed on the torrent site. The user selects a .torrent from the results displayed the file(s) he/she wants to download. Once the .torrent file is downloaded, it is used by a bittorrent program which the user had previously installed. The .torrent file is the set of instructions the program needs to find the files referenced in the .torrent file. The file(s) is downloaded directly from the computer or computers sharing the file. The downloaded file(s) is stored in the area previously designated by the user and/or the software. The downloaded file will remain until moved or deleted.

One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a Bittorrent user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it speeds up the time it takes to download the file.

The computer running the file sharing application, in this case a Bittorrent application has an IP address assigned to it while it is on the internet. Bittorrent users are able to see the IP address of any computer system sharing files to them or receiving files from them. Investigators log the IP address which have sent them files or information regarding files being shared. Investigators can then search public records (ARIN) that are available on the internet to determine the internet service provider who has assigned that IP address. Based upon the IP address assigned to the computer sharing files, subscriber information can be obtained from the internet service provider.

Millions of computer users throughout the world use peer-to-peer (P2P) file sharing networks to share files containing music, graphics, movies and text. These networks have also become a popular way to download and distribute child pornography. Any computer user who can connect to the internet can download P2P application software, which is typically free, and use it to share files through a P2P network.

The BitTorrent network is a very popular and publically available P2P file sharing network. Most computers that are part of this network are referred to as "peers" or "clients". A peer/client can simultaneously provide files to some peers/clients while downloading files from other peers/clients.

The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network client (software) programs, examples of which include the BitTorrent client program, uTorrent client program, and Vuze client program, among others. These client programs are publically available and typically free P2P client software programs that can be downloaded from the Internet.

During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files via automatic uploading[1]. Typically, as users download files or pieces of files from other peers/clients on the BitTorrent network, other users (peers/clients) on the network are able to download the files or pieces of files from them, a process which maximizes the download speeds for all users on the network. Once a user has completed the download of an entire file or files, they can also continue to share the file with individuals on the BitTorrent network who are attempting to download all pieces of the file or files, a process referred to as "seeding".

Files or sets of files are shared on the BitTorrent network via the use of "Torrents". A "Torrent" is typically a small file that *describes* the file(s) to be shared. It is important to note that "Torrent" files do not contain the actual file(s) to be shared, but information about the file(s) to be shared needed to accomplish a download. This information includes things such as the name(s) of the file(s) being referenced in the "Torrent" and the "info hash" of the "Torrent". The "info hash" is a SHA-1[2]hash value of the set of data describing the file(s) referenced in the "Torrent". This set of data includes the SHA-1 hash value of each file piece in the torrent, the file size(s), and the file name(s). The "info hash" of each "Torrent" uniquely identifies the "Torrent" file on the BitTorrent network. The "Torrent" file may also contain information on how to locate file(s) referenced in the "Torrent" by identifying "Trackers". "Trackers" are computers on the BitTorrent network that collate information about the peers/clients that have recently reported they are sharing the file(s) referenced in the "Torrent" file. A "Tracker" is only a pointer to peers/clients on the network who may be sharing part or all of the file(s) referenced in the "Torrent". "Trackers" do not actually have the file(s) but are used to facilitate the finding of other peers/clients that have the entire file(s) or at least a portion of the file(s) available for sharing. It should also be noted that the use of "Tracker(s)" on the BitTorrent network are not always necessary to locate peers/clients that have file(s) being shared from a particular "Torrent" file. There are many publically available servers on the Internet that provide BitTorrent tracker services.

---

[1]As an example, during the downloading and installation of the publically available uTorrent client program, the license agreement for the software states the following: "Automatic Uploading. uTorrent accelerates downloads by enabling your computer to grab pieces of files from other uTorrent or BitTorrent users simultaneously. Your use of the uTorrent software to download files will, in turn, enable other users to download pieces of those files from you, thereby maximizing download speeds for all users. In uTorrent, only files that you are explicitly downloading or sharing (seeding) will be made available to others. You consent to other users' use of your network connection to download portions of such files from you. At any time, you may uninstall uTorrent through the Add/Remove Programs control panel utility. In addition, you can control uTorrent in multiple ways through its user interface without affecting any files you have already downloaded.) thereby maximizing download speeds for all users. In uTorrent, only files that you are explicitly downloading or sharing (seeding) will be made available to others. You consent to other users' use of your network connection to download portions of such files from you. At any time, you may uninstall uTorrent through the Add/Remove Programs control panel utility. In addition, you can control uTorrent in multiple ways through its user interface without affecting any files you have already downloaded.

[2]The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), as a means of identifying files using a digital "fingerprint" that consists of a unique series of letters and numbers. The United States has adopted the SHA1 hash algorithm described herein as a Federal Information Processing Standard. SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols. A file processed by this SHA1 operation results in the creation of an associated hash value often referred to as a digital signature. SHA1 signatures provide a certainty exceeding 99.99% that two or more files with the same SHA1 signature are identical copies of the same file regardless of their file names.

In order to locate "Torrent" files of interest and download the files that they describe, a typical user will use keyword searches on torrent indexing websites, examples of which include *isohhunt.com* and the *piratebay.org*. Torrent indexing websites are essentially search engines that users on the BitTorrent network use to locate "Torrent" files that describe the files they are looking to download. Torrent indexing websites do not actually host the content (files) described by "Torrent" files, only the "Torrent" files themselves. Once a "Torrent" file is located on the website that meets a user's keyword search criteria, the user will download the "Torrent" file to their computer. The BitTorrent network client program on the user's computer will then process that "Torrent" file in order to find "Trackers" or utilize other means that will help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the "Torrent" file. It is again important to note that the actual file(s) referenced in the "Torrent" are actually obtained directly from other peers/clients on the BitTorrent network and not the "Trackers" themselves. Typically, the "Trackers" on the network return information about remote peers/clients that have recently reported they have the same file(s) available for sharing (based on SHA-1 "info hash" value comparison), or parts of the same file(s), referenced in the "Torrent", to include the remote peers/clients Internet Protocol (IP) addresses.

For example, a person interested in obtaining child pornographic images or videos on the BitTorrent network can go to a torrent indexing website and conduct a keyword search using a term such as "preteen sex" or "pthc" (pre-teen hardcore). The results of the keyword search are typically returned to the user's computer by displaying them on the torrent indexing website. Based on the results of the keyword search, the user would then select a "Torrent" of interest to them to download to their computer from the website. Typically, the BitTorrent client program will then process the "Torrent" file. Utilizing trackers and other BitTorrent network protocols, peers/clients are located that have recently reported they have the file(s) or parts of the file(s) referenced in the "Torrent" file available for sharing. The file or files are then downloaded directly from the computer(s) sharing the file or files. Typically, once the BitTorrent network client has downloaded part of a file or files, it may immediately begin sharing the part of the file or files it has with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives "pieces" with the exact SHA-1 hash value of that piece which is described in the "Torrent" file. The downloaded file or files are then stored in an area (folder) previously designated by the user and/or the client program on the user's computer or designated external storage media. The downloaded file or files, including the torrent file, will remain in that location until moved or deleted by the user.

Law Enforcement can search the BitTorrent network in order to locate individuals sharing previously identified child exploitation material in the same way a user searches this network. To search the network for these known torrents can quickly identify targets in their jurisdiction. Law Enforcement receives this information from "Trackers" about peers/clients on the BitTorrent network recently reporting that they are involved in sharing digital files of known or suspected child pornography, based on "info hash" SHA-1 hash values of torrents. These torrents being searched for are those that have been previously identified by law enforcement as being associated with such files. There are BitTorrent network client programs which allow for single-source downloads from a computer at a single IP address, meaning that an entire file or files are downloaded only from a computer at a single IP address as opposed to obtaining the file from multiple peers/clients on the BitTorrent network. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known or suspected child pornography on the BitTorrent network.

During the query and/or downloading process from a suspect BitTorrent network client, certain information may be exchanged between the investigator's BitTorrent client program and the suspect client program they are querying and/or downloading a file from. This information includes 1) the suspect client's IP address; 2) a confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is being reported as shared from the suspect client program; and 3) the BitTorrent network client program and version being utilized by the suspect computer. The law enforcement has the ability to log this information.

The investigation of peer-to-peer file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the Internet Crimes against Children Task Force Program. P2P investigative methodology has led to the issuance and execution of search warrants around the country resulting in the arrest and conviction of numerous offenders possessing and/or distributing child pornography, some of which were also involved in the sexual exploitation of actual child victims.

Sex Offenders

Your Affiant knows that Sex Offenders have specific sexual preferences for prepubescent children. Preferential-type sex offenders are more likely to view, be aroused by and collect theme pornography than Situational Sex Offenders. Child Preferential Sex Offenders receive sexual gratification and satisfaction from actual physical contact with children and from fantasy involving the use of pictures, other photographic art media and writing on or about sexual activity with children.

These offenders collect sexually explicit material consisting of photographs, magazines, films, videotapes, computer depiction, books and slides, which they use for their own sexual gratification and fantasy. These offenders use the sexually explicit material for lowering the inhibitions of children, for sexually stimulating children and themselves and for demonstrating the desired sexual acts before, during and after sexual activity with children.

These offenders rarely if ever dispose of their sexually explicit material, especially when it is used in seduction of their victims and the material is treated as prized possessions. These materials have been found in prior investigations to be concealed on the suspect's person, in safety deposit boxes, private commercial storage spaces, under a home's foundation, in rafters, buried, concealed within vehicles and at places of employment, stored on computer hard drives and other digital storage media and hidden in legitimate books and within video tapes.

These offenders often correspond and or meet with each other to share information and the identities of their victims as a means of gaining status, trust, acceptance and like minded psychological support. These offenders rarely destroy correspondence from each other or victims unless requested to do so and will conceal this material in the same manner as their sexually explicit material.

The majority of these offenders prefer contact with children of one sex in a particular age or development range, peculiar to each individual. These offenders will engage in activities that will be of interest to the type of victims they desire to attract and will provide them with easy access to these children. These offenders take or obtain photographs, film, videotapes or other pictorial media in which the children may be dressed, undressed or engaged in sexual activities alone, with other children and or adults. These items are treasured trophies and are rarely if ever disposed of and will be concealed in the same manner as their sexually explicit material.

These offenders use such pictorial media, as described above, as a means of reliving fantasies or actual encounters with the depicted children. They also utilize these pictorial media as keepsakes and as a means of gaining acceptance status, trust and psychological support by exchanging, trading or selling them to other people with similar interests.

These offenders will cut out pictures of children, usually of the age and sex group they prefer from magazines, newspapers Internet web sites and catalogs. They will also collect videotape excerpts of these children from legitimate television shows and commercials.

These offenders collect all types of media, books, magazines, digital, newspapers and other writings that deal with the subject of sexual activity with children. These people, to reduce the risk of discovery, often maintain and run their own photographic production and reproduction equipment. This may be as simple as the use of instant Polaroid type equipment, video equipment, digital equipment, or as complex as a completely outfitted photo lab.

Offenders will often maintain lists of names, addresses, email addresses and phone numbers of individuals that share the same interests in child sex. This information is sometimes recorded in phone books, address books, scraps of paper, on computer hard drives and other computer media, on answering machines or on audio taping equipment and may be concealed in the same manner as their sexually explicit material.

These people maintain names, addresses, email address and phone number of victim's, victim's friends or victim's of others who have their interest in child sex, including athletic rosters and or school rosters and may conceal them in the same manner as their sexually explicit material.

These offenders often purchase gifts and or give money to their victims and will often record their victims' names on checks, check book registers, credit card slips or statements and other financial records. Offenders may use sex aids such as condoms, dildos, vibrators, lotions, sex dolls, sexual restraints and other sexual apparatus to stimulate their victims and or themselves. These offenders often maintain diaries of their sexual experiences with children and communications with each other. They may take the form of formal diaries, notes or other written formats, or they may be contained on audio tapes, or they may be digitized, such as chat logs and may be concealed in the same manner as their sexually explicit material.

Offenders often collect and maintain artifacts, statues, paintings or other art media which depict children or adults in nude poses or involved in sexual acts. These items are often left or placed where victims can find them to arouse their curiosity or to sexually stimulate them. These offenders often keep mementos of their relationship with specific children as a means of remembrance. These may consist of clothing or other personal items from their victims. Offenders often use drugs or alcohol as a means of inducement to get a child to a particular location such as the offender's home. Both drugs and alcohol are used as a means of seduction reducing the child's inhibitions and for sexual excitement.

These offenders will obtain up to date computer equipment to interconnect with other people on the Internet. They will trade and receive stories, images and information relating to the sexual abuse of children. They will use digital cameras and other image capturing devices to enter images, stories and information into their own computer so that it can be saved or sent to other computer users who share an interest in the sexual abuse of children.

Your Affiant knows through training, knowledge and experience that Child Preferential Sex Offenders will commonly collect and store and protects images of child pornography on their computer systems. Individuals who engage in the collection of child pornography will continue their activity until discovered either by law enforcement or through another reporting agency or persons. Once discovered, they will attempt to elude detection by the destruction of evidence (erasing all digital media), shutting down computer servers or community postings and changing screen names and Internet accounts.

Your Affiant knows through his training, knowledge and experience that subjects engaging in the possession, distribution, purchase, receipt, sale or trade of child pornography will frequently make use of computer equipment to further their activity.

Computers and Internet services enable subjects engaging in the possession, distribution, purchase, receipt, sale or trade of child pornography to communicate with co-conspirators in any region or country with the perception of anonymity. Subjects who view or collect child pornography value their collections and often go to great lengths to organize and protect their collections including concealing the images on computer media. Your Affiant also knows through training, knowledge and experience that when subjects possessing child pornography conceal or delete it to avoid detection that it is possible to recover files and data from computer media in hidden areas or after it has been deleted.

Computer/Wireless

Your affiant knows that modern residential computers often operate utilizing wireless routers. A wireless router is a device that performs the functions of a router but also includes the functions of a wireless access point and a network switch. They are commonly used to allow access to the Internet or a computer network without the need for a cable or phone connection. It can function in a wired LAN (local area network), a wireless only LAN (WLAN), or a mixed wired/wireless network. With all wireless routers, the strength and speed of the signal being transmitted varies greatly based on distance and other factors, such as the types of obstacles that lie between the computer and the wireless router that may cause interference.

Wireless communications also raise security concerns because they are vulnerable to intentional and accidental interception, an act described colloquially as "piggybacking." Piggybacking refers to access to a wireless Internet connection by bringing one's own computer within the range of another's wireless connection, and using that service without the subscriber's explicit permission or knowledge. These facts make it relevant to determine if the wireless network is password protected, although it is still feasible to defeat certain password protected systems. Although this is possible, your Affiant knows that it is rare for this to occur. Regardless of the system security, it is important to note that wireless routers maintain addressing data associated with the computer devices that access them. For example, a Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment of a wireless network. MAC addresses are used for numerous network technologies and most network technologies including Ethernet. Logically, MAC addresses are used in the Media Access Control protocol sub-layer of the standardized OSI reference model. MAC addresses are most often assigned by the manufacturer of a network interface card (NIC) and are stored in its hardware, the card's read-only memory, or some other firmware mechanism.
If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the burned-in address. It may also be known as an Ethernet hardware address (EHA), hardware address or physical address.

The evidence linking a computer to the distribution of child pornography, I know that when a user saves a file to the computer's hard drive or other storage media, the system assigns the data to specific clusters or locations on the media, which are then reserved. The event may also be recorded in other files on the computer such as .dat and link files. If the user later deletes a file, the data is not actually erased, but rather the system marks those previously reserved clusters as once again being available for use.
The original data is still intact on the media. The data is recoverable until it is overwritten either by the use of a "wiping" program or when new files are saved and assigned the same clusters. The process of overwriting may not eradicate the entire file, leaving portions available for recovery.

It is therefore possible that data related to the possession of a file can be recovered for an extended period of time after "deletion," even months or years later. Until the data is overwritten, it is still in a recoverable state.

This data can therefore assist in establishing possession, receipt, and distribution of images of child pornography."

Wherefore, your Affiant requests that a Search and Seizure Warrant be issued for said residence known as **309 Raleigh Road Glen Burnie, MD 21061.**

I solemnly affirm under the penalties of perjury and upon personal knowledge that the contents of the foregoing Application and Affidavit are true. For any portion of the Application and Affidavit that relies upon information provided by someone other than the applicant, and only for such portion(s), I solemnly affirm under the penalties of perjury that the contents of the foregoing Application and Affidavit are true to the best of my knowledge, information and belief.

Affiant ____________________
Detective J. Rees #4648

16-1301SAG

DISTRICT COURT OF MARYLAND
FOR BALTIMORE COUNTY

SEARCH AND SEIZURE WARRANT

TO: Any Police Officer of Baltimore County, Maryland

GREETINGS:

WHEREAS:

An application and affidavit were made and delivered to me by Detective J. Rees #4648, a sworn member of the Baltimore County Police Department, who has reason to believe that:

ON THE PREMISES KNOWN AS:

309 Raleigh Road Glen Burnie, MD 21061 (Anne Arundel County)

Described as:
A single family residence with gray siding, black shutters, and a white front door. There are no numerical markings on the home, however it is situated directly between houses marked 311 and 307. The residence is currently secured by Baltimore County Police Detectives and is known by sight to your Affiant.

there is presently concealed certain property, NAMELY:

A. **Seize and examine any and all cell phones**
B. **Seize any documents, envelopes, cancelled checks, or papers in the name of occupants that establishes occupancy.**
C. **Seize and examine address books, advertisements, brochures, catalogs, correspondence, documents, electronic organizers, mailing lists, notes, organizers, publications, receipts, records that may indicate the distribution, barter, purchase, receipt, sale or trade of child pornography.**
D. **Seize and examine any documents, notes, papers or other items containing chat logs, E-mail addresses, E-mail messages, Internet Service Provider information, IP addresses, passwords, Uniform Resource Locator addresses and user profiles.**
E. **Seize and examine any books, DVD, magazines, motion picture film of any format, negatives, photographs, printed images generated by computer, slides, undeveloped film of any format and videocassettes that may contain child pornography.**
F. **Seize and examine any electronic media including, but not limited to Media Cards and Flash Based memory that may contain evidence of the distribution, production, receipt, transmission or viewing of child pornography stored in any format.**

G. Seize and exam any and all portable media players (PMP), a consumer electronics device that is capable of storing and playing digital media. The digital media is typically stored on a hard drive, microdrive, or flash memory. PMPs are capable of supporting digital audio, digital images, and digital video. Usually, a color liquid crystal display (LCD) or organic light-emitting diode (OLED) screen is used as a display. Various players include the ability to record video, usually with the aid of optional accessories or cables, and audio, with a built-in microphone. Some players include readers for memory cards, which are advertised to equip players with extra storage or transferring media.

H. Seize and examine any magnetic media including, but not limited to hard drives, floppy diskettes and tapes of any format that may contain evidence of the distribution, production, receipt, transmission or viewing of child pornography stored in any format.

I. Seize and examine any optical media including, but not limited to CD's, DVD's and Blu-rays of any format that may contain evidence of the distribution, production, receipt, transmission or viewing of child pornography stored in any format.

J. Seize and examine any computer hardware capable of analyzing, collecting, concealing, converting, displaying, receiving or transmitting data electronically, magnetically or optically. This hardware includes, but is not limited to central processing units, portable computers (i.e. laptop computers), file servers, peripheral input/output devices (i.e. keyboards, plotters, pointing devices, printers, scanners and video display monitors), storage devices capable of reading and/or writing to computer media (i.e. electronic, magnetic or optical), communications devices (i.e. modems, cable modems, network adapters and wireless communication devices), any devices or parts used to restrict access to computer hardware (i.e. keys and locks) and any other piece of equipment necessary to duplicate the functionality of the hardware at the time of seizure (i.e. batteries, cables, instruction manuals and power cords) that may be used in the distribution, production, receipt, transmission or viewing of child pornography.

K. Seize and examine any computer software stored electronically, magnetically, or optically that may be used to facilitate the distribution, production, receipt, transmission or viewing of child pornography and any instruction manuals associated with the software.

L. To seize and examine any cameras, digital cameras, motion picture cameras, video cameras, web cameras and any associated accessories (i.e. backdrops, batteries, carrying cases, instruction manuals, lenses, lighting equipment, meters, remote controls and tripods) that may be used in the production of child pornography.

M. Open any containers, envelopes, boxes, packages, safes to examine the contents and seize any of the aforementioned items, which is evidence relating to the commission of a crime of crime of Child Pornography in violation of in violation of Maryland Annotated Code, Criminal Code, Article CR 11-207 and 11-208, and I am satisfied that there is probable cause to believe that the property described is in the location above described and that probable cause for issuance of the Search and Seizure Warrant exists, as stated on the Application and Affidavit attached to this warrant.

You are, therefore, commanded, with the necessary and proper assistance, to (1) search the place herein above specified; (2) if the property named in the Application and Affidavit is found there, to seize it; (3) seize any evidence of the commission of a misdemeanor or felony by a person therein; (4) seize any evidence of the commission of a misdemeanor or felony which is found in the building, apartment, premises, places, or things covered by this warrant; (5) leave a copy of this Warrant and Application/Affidavit with an inventory of the property seized pursuant to applicable law and (6) return a copy of this Warrant, Application/Affidavit, and inventory, if any, to me within ten (10) days after execution of this Warrant; or, if not served, to return this Warrant and Application/Affidavit to me promptly, per Maryland Rules, Rule 4-601(h).

Dated this 17 day of March, 2016 at 11:26 a.m./p.m.

SIGNED: [signature]
JUDGE